International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Review on Privacy-Conserving Public Auditing for Shared Data in Cloud Computing, with a Focus on User Revocation

Mahesh Shinde[1], Y.B.Gurav[2]

[1]ME Research Scholar, Padmabhushan Vasantdada Patil Institute of Technology, Pune, Maharashtra India

[2]Professor, H.O.D. Dept of Computer Engineering, Padmabhushan Vasantdada Patil Institute of Technology, Pune, Maharashtra India

Abstract: ***The term cloud computing has been emerged as a computing network over the Internet. Cloud data indulge storing of the data in the cloud as well as has sharing capability among multiple users. Due to failures of human or hardware and even Software errors cloud data is associated with data integrity. Several mechanisms have been proposed in order to allow both the data owners as well as the public auditors to audit cloud data integrity efficiently without retrieving the entire data from the cloud servers. A Third Party Auditor (TPA) will perform integrity checking and the identity of the signer on each block in shared data is kept private from them. In this paper, we only survey for auditing the integrity of shared data in the cloud with efficient user revocation while still conserving identity privacy.***

Keywords: Public auditing, privacy-conserving, shared data, user revocation, cloud computing.

1. Introduction

Cloud computing is Internet-based computing, whereby shared resources, software, and information are provided to computers and other devices on demand. It describes a new supplement, consumption, and delivery model for IT services based on the Internet. It has been envisioned as the next generation information technology (IT) architecture for enterprises, due to its wide range of unprecedented advantages in the IT history: on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk. As a disruptive technology with profound implications, Cloud Computing is transforming the very nature of how businesses use information technology. One fundamental aspect of this paradigm shifting is that data is being centralized or outsourced to the Cloud. From users' perspective, including both individuals and IT enterprises, storing data remotely to the cloud in a flexible on-demand manner brings appealing benefits: relief of the burden for storage management, universal data access with location independence, and avoidance of capital expenditure on hardware, software, and personnel maintenances, etc.

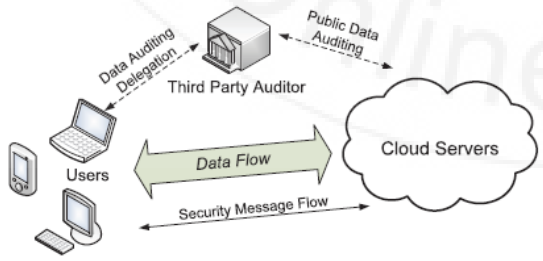

Fig. 1. The architecture of cloud data storage service.

While Cloud Computing makes these advantages more appealing than ever, it also brings new and challenging security threats towards users' outsourced Data. The data integrity of shared data in the cloud may still be compromised. Third Party Auditor is kind of inspector.

Which audits the data integrity on the behalf of cloud service provider without retrieving total data? It challenges the cloud server for the correctness of data storage while keeping no private information. To let off the burden of management of data of the data owner, TPA will audit the data of client. It extinguish the involvement of the client by auditing that whether her data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. Then it relinquishes the audit report which would help owners to evaluate the risk of their subscribed cloud data services, and it will also be beneficial to the cloud service provider to improve their cloud based service platform. In this way TPA will help data owner as well as users to make sure that his data are safe in the cloud and management of data will be less burdening to data owner. Therefore, to enabling a privacy-preserving third party Auditing protocol, independent to user revocation, is the problem we are going to tackle in this paper. Our review is among rare ones to support privacy-preserving public auditing in cloud computing, with a focus on user revocation.

The rest of this paper is organized as follows: We first provided Literature survey in section 2. Then section 3 discussed the problem definition. Section 4 provided the proposed scheme and section 5described the conclusion and future work.

2. Literature Survey

[9]To introduce the TPA effective safely, the audit process should not compensate an additional fee for online users and carry-in; there is no new compromise to the privacy of user data. This proposed approach is a secure cloud storage

Licensed Under Creative Commons Attribution CC BY

mechanism as public auditing mechanism for secure cloud storage. At the same time this approach extends to the TPA performance to audit multiple users efficiently. By showing high efficiency and provable security and performance analysis a wide range of security, the proposed scheme.

[6]They have utilized the idea of proxy re-signatures to allow the cloud to re-sign blocks on behalf of existing users during user revocation, so that existing users need not to download and re-sign blocks by themselves. Moreover, this mechanism is able to support batch auditing by verifying multiple auditing tasks simultaneously. Experimental results show that the mechanism can significantly improve the efficiency of user revocation.

[12] They have exploit ring signatures to compute the verification information needed to audit the integrity of shared data. With this mechanism, the identity of the signer on each block in shared data is kept private from a third party auditor (TPA), who is still able to publicly verify the integrity of shared data without retrieving the entire file.

[5] This system proved the data freshness (proved the cloud possesses the latest version of shared data) while still preserving identity privacy. An experimental result of this ensures that retrieved data always reflects the most recent updates and prevents rollback attacks.

[3] The main problem associated with [12] is the size of signatures and verification time linearly increase with the number of users in the group that is solved with Knox considering audit of the data integrity which is to be shared with a large group while still preserving identity privacy from the TPA by leveraging group signatures.

3. Problem Statement

With relinquish trends in cloud, Data integrity is one of the critical issue, as there is lack of identity privacy, where the users are unacquainted with the auditor of the data, over geographically scattered datacenters. This features of cloud computing evolved various concerns related to user's identity, data integrity and users availability. Ultimately this influences to propose an enhanced model in order to audit the data integrity and keeping the identity privacy with efficient user revocation while sharing.

4. Proposed System

Examining the above research work we have proposed a new method through which we not only audit the data integrity but also conserve identity privacy with user revocation. Our proposed mechanism should posses the following Properties:

1) **Correctness**: The TPA should be correctly check the Integrity of shared data correctly.
2) **Efficient User Revocation**: When a user is revoked from the group, the blocks signed by that user can be re-signed efficiently. As well as, only existing members in the group can only generate valid signatures on shared data and the members which are revoked from the group cannot compute the valid signatures on shared data.
3) **Public Auditing**: The Third Party Auditor the integrity of shared data can be audit by Third Party Auditor without retrieving the entire data from the cloud, even if some blocks in shared data have been re-signed by the cloud.

For achieving these properties we are going to use some predefined cryptographic primitives.

Proxy re-signatures
A Semi-trusted proxy acts as a translator of signatures between two users first proposed by Blaze et al. [10], More Briefly, the proxy converts a signature of one user into a signature of other user on the same block. Without knowing any private keys of the two users, which means that it cannot sign any block on behalf of any user. In this paper, we have improved the efficiency of user revocation, by acting cloud as a proxy and convert those signatures during user revocation.

Ring Signatures
The ring signatures concept is first proposed by Rivest et al. [4] in 2001. With ring signatures, a verifier is convinced that a signature is computed using one of group member's private keys, but the verifier is not able to determine which one. This property can be used to preserve the identity of the signer from a verifier.

We have reviewed that the following algorithms will help us to construct our proposed mechanism.
KeyGen:
In KeyGen each user in the group generates her public key and private key.
ReKey:
For each pair of user in the group , cloud computes a resigning key with ReKey.
ProofGen:
Proof of possession of shared data is generated.
ProofVerify:
In ProofVerify TPA verifies the correctness of proof responded by cloud.
ReSign:
In ReSign algorithm signature of revoked user is converted to the original user.
RingSign:
In a RingSign a user in the group signs a block with their private key & all group members public key.
RingVerify:
In this verifier is allowed to check whether the given block is signed by that the group member only.

Homomorphic verifiable tags:
These are the basic tools to construct data auditing mechanisms. Besides user with a private key which generates the valid signatures, a homomorphic authenticable signature scheme denotes a homomorphic authenticator based on signatures, which also satisfies the Blockless verification and Non-malleability.

Discussing in details to our auditing mechanism.

Licensed Under Creative Commons Attribution CC BY

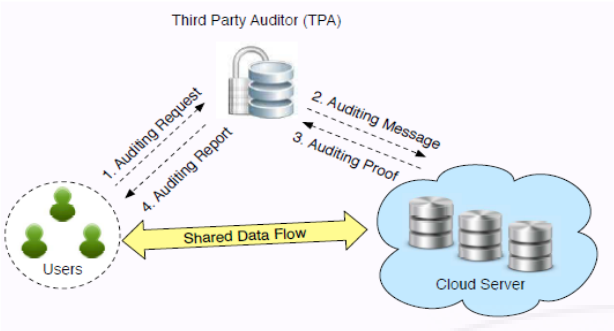

Fig. 2. Our system model includes the cloud server, the third party auditor and users.

A user (original user or a group user) who wants to verify the integrity of shared data first sends an auditing request to the TPA. On receiving that auditing request, TPA sends an auditing message to the cloud server, and gets an audit proof of shared data from the cloud server. Then the TPA confirms the correctness of the auditing proof. Eventually, the TPA conveys an auditing report to the user based on that result of the verification.

It includes with nine algorithms: **KeyGen**, **SigGen**, **Modify ReKey**, **ReSign, RingVerify, RingSign, ProofGen** and **ProofVerify**. In **KeyGen**, users generate their own public/private key pairs. In **ReKey**, the cloud computes a re-signing key for each pair of users in the group. He/she computes a signature on each block as in **Sign**. After that, if a user in the group modifies a block in shared data, the signature on the modified block is also computed as in **Sign**. In **ReSign**, a user is revoked from the group, and the cloud re-signs the blocks, which were previously signed by this revoked user, with a resigning key. In **SigGen**, a user (either the original user or a group user) is able to compute ring signatures on blocks in shared data. Each user in the group is able to perform an insert, delete or update operation on a block, and compute the new ring signature on this new block in **Modify**. The verification on data integrity is performed via a challenge-and-response protocol between the cloud and a public verifier. More specifically, the cloud is able to generate a proof of possession of shared data in **ProofGen** under the challenge of a public verifier. In **ProofVerify**, the TPA verifies the proof and sends an auditing report to the user. Before the original user outsources shared data to the cloud, she decides all the group members, and computes all the initial ring signatures of all the blocks in shared data with her private key and all the group members' public keys. After shared data is stored in the cloud, when a group member modifies a block in shared data, this group member also needs to compute a new ring signature on the modified block. In **ProofVerify**, a public verifier is able to check the correctness of a proof responded by the cloud. In **ReSign**, without loss of generality, we assume that the cloud always converts signatures of a revoked user into signatures of the original user. The reason is that the original user acts as the group manager, and we assume he/she is secure in our mechanism. Another way to decide which re-signing key should be used when a user is revoked from the group is to ask the original user to create a priority list (PL). Every existing user's id is in the PL and listed in the order of re-signing priority.

When the cloud needs to decide which existing user the signatures should be converted into, the first user shown in the PL is selected. To ensure the correctness of the PL, it should be signed with the private key of the original user (i.e., the group manager).

5. Conclusion and Future Work

Now a day's IT Infrastructure is propelling towards cloud computing, but the data integrity concerns with identity privacy which must be addressed. In this paper, we reviewed various privacy preserving mechanisms for static group in cloud computing and propose a new idea for identity privacy with efficient user revocation in cloud computing environment. We have furnished the simulated implementation of HAPS [6] and HARS [12] algorithms. Presently this research is under development to find the system for preserving identity privacy for revocation of the user or group member while sharing the data on cloud.

In future work we would be focusing on developing a complete framework that would cover all integrity aspects related to data with identity privacy for dynamic group. We thought this channelized project would lean to aid the institutions/organizations to encourage towards the Cloud environment and construct rich IT infrastructure.

References

[1] John W. Rittinghouse James F. Ransome, "Cloud Computing Implementation, Management, and Security", CRC Press Taylor & Francis Group 6000 Broken Sound Parkway NW, Suite 300 Boca Raton, FL 33487-2742 © 2010 by Taylor and Francis Group, LLC CRC Press is an imprint of Taylor & Francis Group, an Informa business.
[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," in Proc. ACM Conference on Computer and Communications Security (CCS), 2007, pp. 598–610.
[3] B. Wang, B. Li and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud", ACNS2012
[4] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," in the Proceedings of IEEE INFOCOM 2010, 2010, pp. 525–533.
[5] P. Maheswari, B. Sindhumathi "AFS: Privacy-Preserving Public Auditing With Data Freshness in the Cloud" IOSR Journal of Computer Engineering (IOSR-JCE) PP 56-63
[6] B. Wang, B. Li, and H. Li, "Panda: Public Auditing For Shared Data with Efficient User Revocation in The Cloud" IEEE Trans. Services Computing, Dec.2013
[7] R. L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," in Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). Springer-Verlag, 2001, pp. 552–565

Licensed Under Creative Commons Attribution CC BY

[8] R. L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," in Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). Springer-Verlag, 2001, pp. 552–565.
[9] Lakshmi et al., International Journal of Advanced Research in Computer Science and Software Engineering 4(8), August - 2014, pp. 54-62
[10] M. Blaze, G. Bleumer, and M. Strauss, "Divertible Protocols and Atomic Proxy Cryptography," in the Proceedings of EUROCRYPT 98. Springer Verlag, 1998, pp.127–144
[11] Zahir Tari, RMIT University, "Security and Privacy In Cloud Computing", IEEE Cloud Computing Published by the IEEE Computer Society 2014
[12] B. Wang, B. Li, and H. Li, "Oruta: Privacy- Preserving Public Auditing for Shared Data in the Cloud," in the Proceedings of IEEE Cloud 2012, 2012, pp. 295–302
[13] Zhifeng Xiao and Yang Xiao, Senior Member, IEEE, "Security and Privacy in Cloud Computing", IEEE Communications Surveys & Tutorials, vol. 15, no. 2,Second quarter 2013.
[14] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," in Proc. IEEE International Conference on Computer Communications (INFOCOM), 2010, pp. 525–533
[15] http://techatftc.wordpress.com/2012/05/15/what- does-it mean-to-preserve-privacy/

Author Profile

Prof. Y B. Gurav Presently working in Padmabhushan Vasantdada Patil Institute of Technology, Pune, Maharashtra, India affiliated to University of Pune. He has working experience of 16 Years. His fields of interest are Cloud Computing and Data Mining.

Mr. Mahesh Shinde received B.E (Computer) from Pravra Rural Engineering College Loni, Maharashtra, India affiliated to University of Pune in the year 2012 and Pursuing M.E degree at Padmabhushan Vasantdada Patil Institute Of Technology, Pune, Maharashtra, India affiliated to University of Pune. His Fields of interest are Cloud Computing and Data Mining.

Licensed Under Creative Commons Attribution CC BY